IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NORTH CAROLINA
WESTERN DIVISION

No. 5:16-CR-201-FL-1

UNITED STATES OF AMERICA,	)	
	)	
	)	
v.	)	ORDER
	)	
	)	
KEITH WILLIAM DEICHERT	)	
	)	
Defendant.	)	

This matter is before the court on defendant's motion to suppress certain evidence allegedly obtained in violation of the Fourth Amendment to the United States Constitution and Rule 41 of the Federal Rules of Criminal Procedure. (DE 21). For the reasons that follow, defendant's motion is denied.

BACKGROUND

August 23, 2016, a grand jury returned an indictment charging defendant with 10 counts of manufacturing child pornography, in violation of 18 U.S.C. § 2251 (a) & (e), 10 counts of receiving child pornography, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B).

November 7, 2016, defendant filed the instant motion to suppress. Defendant moves to suppress all evidence seized electronically from defendant's home computer February 20, 2015, through a computer forensic tool the Federal Bureau of Investigation ("FBI") terms a network investigative technique ("NIT"), described in detail below. Additionally, defendant moves to

suppress fruits of that search including computer equipment seized from defendant's home October 29, 2015, and electronic data found therein.

In support of his motion, defendant asserts that the government violated his rights under the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure when it deployed the NIT pursuant to an allegedly invalid search warrant issued February 20, 2015, by a magistrate judge sitting in the Eastern District of Virginia. Defendant contends the warrant was unsupported by probable cause, constituted an anticipatory warrant that never properly was triggered, violated the Fourth Amendment particularity requirement, and issued in violation of Rule 41.

STATEMENT OF FACTS

Facts pertinent to the instant motion may be summarized as follows. Prior to February 20, 2015, a resident of Naples, Florida ("Playpen's administrator") began operating a website known as "Playpen," which constituted an online message board that hosted illicit images and videos and enabled users to share child pornography. Additionally, Playpen contained information about how to maintain anonymity while engaged in conduct related to child pornography, including advice about online privacy and guidance for handling child victims.

Playpen's administrator took extensive security measures to evade law enforcement and to protect users' anonymity. In particular, Playpen was inaccessible to ordinary internet users. Playpen was accessible only through "the onion router" ("Tor"), which is a system that appears to users as a standard internet browser but is designed to conceal users' internet protocol ("IP") addresses and other identifying information. Tor achieves this result by routing online communications through numerous connected computers ("nodes"). This process creates the appearance that the last node in the chain ("exit node") is the only other party to a communication.

In reality, the nodes are unable to access the content of a communication transmitted through Tor, nor is it possible for an observer to retrace the steps in the chain to determine the IP address of the computer that initiates communication ("activating computer").

One court has offered the following useful analogy to describe the process by which Tor conceals users' identities:

> Imagine that "John receives a locked box, for which he has the key. He opens it, finding within another locked box, labeled "Jane." He does not have the key for Jane's box, so he mails the box to Jane. Jane has the key and within she finds a locked box labeled "Jack." She does not have the key for Jack's box, so she mails it to Jack. Jack likewise opens his box, finds within a locked box labeled 'Jill,' and mails that box to Jill. Jill opens her box to find an envelop bearing a website's address. She writes her own address as the return address and mails the letter. This process is reversible, so information from a website can return through the Tor network to the end user. Nor does John, Jane, Jack, or Jill know who is communicating with whom."

United States v. Knowles, No. 15-cr-875, 2016 WL 6952109, at *1, *5 (D.S.C. Nov. 28, 2016). By this process, a website's host knows the IP address only of the exit node, i.e, the return address of the last letter in the illustration above. Additionally, because each node sends no information about the complete return path, it is impossible to identify the activating computer simply by controlling a website accessed through Tor.

Beginning December 2014, Playpen's administrator inadvertently made Playpen available on the open (non-Tor) internet for a number of days. During this time, the FBI was able to locate Playpen's servers, seized them, and move the servers to a location within the Eastern District of Virginia. The Tor network would have made it impossible to identify Playpen's users absent special methods.

To address this problem, the FBI obtained a warrant ("NIT warrant") from a magistrate judge in the Eastern District of Virginia that permitted the FBI to continue operating Playpen for 30 days.

The warrant also permitted the FBI during that time to deploy its NIT directed to the computer of any user who entered a username and password to log into Playpen. Nothing in the record discloses the NIT's full capabilities, but, at a minimum, the NIT is capable of installing itself on a target's computer, running covertly in the background, and causing a user's computer to send directly to the FBI information that is normally concealed by Tor. In this case, the warrant authorized the FBI to gather information consisting of

- the IP address for any activating computer that logged into Playpen;
- a unique identifier generated by the NIT to distinguish data received from each activating computer;
- the type of operating system running on each activating computer;
- information indicating whether the NIT already had been installed on an activating computer;
- the host name for each activating computer, which is a unique set of characters that serves to identify computers connected to a network;
- the operating system username active on each activating computer; and
- the media access control address ("MAC address") for each activating computer, which is another set of characters that is designed to identify uniquely certain equipment used to facilitate communication over an electronic network.

(DE 21-3 at 25–26). The NIT warrant set forth no limitation on the number of computers on which the NIT was to be installed. The NIT warrant authorized the FBI to deploy the NIT against any activating computer that logged into Playpen. (DE 21-2 at 2).

On February 26, 2015, FBI agents noted that a user logged into Playpen under the username "harris." (DE21-5 at 30). Pursuant to the NIT warrant, the FBI deployed its NIT to obtain the information described above. The NIT revealed that the subject's computer was assigned IP address

174.97.169.226. Using publicly available websites, the FBI determined that Time Warner Cable provided internet access to that IP address. Accordingly, it served upon Time Warner Cable an administrative subpoena to obtain the name and address of the corresponding user. In response, Time Warner Cable submitted records indicating that defendant was the user in question. The same records provided the address of defendant's home in Raleigh, North Carolina. Using this information, the FBI obtained from a magistrate judge in this district a warrant ("EDNC warrant") to search and seize defendant's computer equipment. The FBI executed the EDNC warrant October 29, 2015, and after a forensic examination of defendant's computer equipment, found evidence tending to suggest that defendant possessed, distributed, and manufactured child pornography. Indictment followed.

DISCUSSION

Defendant advances four challenges to the validity of the NIT warrant. First, defendant contends the NIT warrant was not supported by probable cause. Second, defendant contends the NIT warrant constituted an anticipatory warrant that was never properly triggered. Third, defendant contends the NIT warrant did not describe the place to be searched with adequate particularity. Finally, defendant contends that the magistrate judge issued the NIT warrant in violation of Federal Rule of Criminal Procedure 41(b). With respect to each point, defendant contends that no exception to the exclusionary rule applies.

Defendant's first three challenges sound in the Fourth Amendment to the Constitution, while the last arises under a rule of criminal procedure. The court addresses defendant's Fourth Amendment challenges before turning to his contentions under Rule 41.

A. Probable Cause

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . ." U.S. Const. amend IV. Ordinarily, a "search . . . is 'unreasonable' unless it has been authorized by a valid search warrant, and in cases in which the Fourth Amendment requires that a warrant to search be obtained, 'probable cause' is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." United States v. DeQuassie, 373 F.3d 509, 518 (4th Cir. 2004) (quoting Camera v. Muni. Ct. of San Francisco, 387 U.S. 523, 528–29 (1967)).

"Probable cause exists where the facts and circumstances within [officers'] knowledge and of which they had reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed." Brinegar v. United States, 338 U.S. 160, 175 (1949) (alterations omitted); see also United States v. Doyle, 650 F.3d 460, 475 (4th Cir. 2011). "The proponent of a motion to suppress has the burden of establishing that his Fourth Amendment rights were violated by the challenged search or seizure." Rakas v. Illinois, 439 U.S. 128, 130 n.1 (1978) (internal citations omitted). Courts accord great deference to a magistrate judge's initial determination of whether probable cause to search exists, asking only whether there was a substantial basis for determining the existence of probable cause." United States v. Monteith, 662 F.3d 660, 664 (4th Cir. 2011). Accordingly, probable cause is not vitiated where a magistrate judge issues a warrant in reliance upon an affidavit submitted in support of a warrant application unless the affiant omits or falsifies a material fact and such omission or falsehood is intentional or the product of reckless disregard for the truth. United States v. Shorter, 328 F.3d 167, 171 (4th Cir. 2003).

The NIT warrant authorized the FBI to deploy the NIT and thereby search computers used by anyone who entered a username and password to log into Playpen. (DE 21-2 at 2). Therefore, to find that the NIT warrant was supported by probable cause, there must exist sufficient reason to conclude that anyone who logged into Playpen by entering a username and password did so with intent to commit a criminal offense, such as gaining possession of or sharing child pornography. See Doyle, 650 F.3d at 475. Sufficient reason to draw such a conclusion might exist if an officer could see that its login page standing alone provided sufficient notice of Playpen's illegal content, or if an officer reasonably believed that users could not reach Playpen except after taking steps that render it impossible to stumble upon Playpen without intent to engage in illegal activity. See id.

In light of the foregoing observations, defendant argues that two factual assertions contained in the NIT warrant application and supporting affidavit ("NIT affidavit") cast doubt upon the magistrate judge's probable cause finding. First, the NIT affidavit inaccurately describes the version of Playpen's login page that displayed to users at the time the FBI filed the NIT warrant application. Specifically, where the NIT affidavit asserts that Playpen's login page displayed images of "partially clothed prepubescent females with their legs spread apart," Playpen's login page actually displayed a single suggestively dressed, but fully clothed, female with her legs crossed in a risqué, though less sexually explicit manner than described in the application. (Compare DE 26-5 with DE 21-6).[1] Additionally, simply viewing the latter image does not immediately disclose that the depicted female is prepubescent or even underage. Therefore, because the login page that actually displayed to users at the time the FBI submitted the NIT warrant application and during the NIT warrant's 30 day

[1] The image, as described in the NIT warrant application, was, in fact, featured on Playpen's login page until February 19, 2014, the day before the FBI submitted the NIT warrant application. (DE 21 at 9).

window does not indicate unambiguously that Playpen is a child pornography website, the magistrate judge's probable cause finding, if correct, must rest upon other ground.

The NIT affidavit states that "[b]ecause [Playpen] is a Tor hidden service, it does not reside on the traditional or 'open' internet . . . a user must know the web address of the website in order to access the site." (DE 21-3, ¶ 10). The import of the foregoing statement is that if it is impossible to stumble upon Playpen without obtaining Playpen's web address through word of mouth or other intentional means, then it is permissible to infer that every individual who logged into Playpen did so with knowledge of Playpen's content and intent to download or share child pornography. See Doyle, 650 F.3d at 475.

In the instant case, defendant disputes the affiant's account. That is, where the affiant claims that it is virtually impossible to reach a Tor hidden service such as Playpen through a search engine, defendant claims that Tor search engines do exist and could lead an innocent browser to Playpen's login page.

Defendant's evidence that Tor search engines exist does not, however, undermine the magistrate judge's probable cause finding. As set forth in Brinegar,"[p]robable cause exists where the facts and circumstances within [officers'] knowledge[,]" justify a belief that evidence of a crime will be found in a particular place. 338 U.S. at 175 (emphasis added). In this manner, even if Playpen was reachable through a Tor-based search engine, the affiant's failure to bring such information to the magistrate judge's attention does not support suppression unless the affiant's omission was intentional or the product of reckless disregard for the truth. Shorter, 328 F.3d at 171.

Defendant has submitted no evidence to support a contention that the NIT affidavit was deficient due to intentional or reckless omissions of fact.[2]

Therefore, where no evidence of record supports a finding that the FBI intentionally or recklessly omitted information about Tor-based search engines from the NIT affidavit, defendant's contention that the magistrate judge should have denied the NIT warrant application on the ground that an innocent browser could have reached Playpen through a Tor-based search engine is unavailing. Accordingly, in light of the standards set forth in Brinegar and Shorter, defendant has not met his burden to demonstrate that the magistrate judge's probable cause finding was in error. See Brinegar, 338 U.S. at 175; Shorter, 328 F.3d at 171. The court turns its attention below to another of defendant's arguments that the warrant was invalid.

B. Anticipatory Warrant

"An anticipatory warrant is a warrant based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of crime will be located at a specified place." United States v. Grubbs, 547 U.S. 90, 94 (2006). An anticipatory warrant subjects its execution to a "triggering condition," which establishes probable cause. Id. Therefore, if the relevant triggering condition does not occur, the Fourth Amendment prohibits authorities from executing an anticipatory warrant. See id.

As described in the court's foregoing probable cause analysis, probable cause existed to search the computer of anyone who logged into Playpen because, based on information available

[2] Moreover, defendant has not requested a hearing to gather evidence regarding the circumstances of the FBI's failure to acknowledge the existence of Tor-based search engines in the NIT affidavit. See Franks v. Delaware, 438 U.S. 154, 155–56 (1978) (holding that a criminal defendant may request a hearing to demonstrate intentional or reckless falsity of information contained in an affidavit submitted in support of a warrant application if the defendant can make a preliminary showing that the affidavit in question contained materially false information).

to officers at the time, it was impossible to reach Playpen without obtaining its exact web address through word of mouth or other intentional means. Therefore, it was reasonable to believe that anyone who took the necessary steps in reaching Playpen knew its contents and would not have logged into Playpen absent intent to commit a crime. See Brinegar v. United States, 338 U.S. 160, 175. Accordingly, because the foregoing circumstances indicate that logging into Playpen establishes probable cause, the fact that the NIT warrant treats the act of logging into Playpen as its triggering condition is not unconstitutional. See Grubbs, 547 U.S. at 94.

In support of a contrary argument defendant contends that, because images on Playpen's login page changed between the time NIT warrant was granted and the time the FBI deployed the NIT against defendant, the relevant triggering condition never occurred. Specifically, defendant contends that the NIT warrant's triggering condition was not satisfied because, where Playpen's login page, standing alone, did not unabashedly announce that Playpen was a child pornography site, probable cause did not exist to search every user who logged in. However, this argument is unavailing because, as set forth above, probable cause existed where accessing Playpen required users to obtain Playpen's exact web address through word of mouth or other intentional means. Therefore, to the extent defendant challenges the NIT warrant on the ground that its triggering condition never occurred, defendant's claim is denied.

C. Particularity

In addition to the requirement of probable cause, the Fourth Amendment commands that every warrant "particularly describ[e] the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. A warrant application describes places to be searched with

sufficient particularity if an officer "can, with reasonable effort ascertain and identify the place intended." U.S. v. Blackwood, 913 F.2d 139, 141 n. 1 (4th Cir. 1990) (citing Steele v. U.S., 267 U.S. 498, 503 (1925)).

Under the heading "[p]lace to be [s]earched" the warrant application requests authorization to use the NIT to obtain information from activating computers whose users log into Playpen. (DE 21-2). Specifically, the warrant authorized the FBI to gather information including activating computers' IP address, operating system, host name, MAC address, and a unique identifier used to distinguish data received from other activating computers targeted by the NIT.

Based on the test set forth in Blackwood and Steele and in light of the extensive detail in which the supporting affidavit describes the FBI's intended use of the NIT, it is clear that an officer with the NIT warrant in hand easily could identify the authorized place to be searched. Specifically, regardless of whether the place to be searched is characterized as the Playpen servers hosted in the Eastern District of Virginia, or as any computer used to log into Playpen, there is no difficulty in determining from the text of the warrant where and under what conditions an officer executing the NIT warrant may look for incriminating evidence.

Defendant emphasizes, however, that the NIT warrant potentially authorizes searches against an indefinite number of individuals and that the FBI could have sought authorization to deploy the NIT more narrowly. Additionally, defendant reiterates his contention that the NIT warrant was unsupported by probable cause. Both arguments fail.

First, as set forth above, the NIT warrant was supported by probable cause. Second, rather than naming individual computers to be searched, the NIT warrant describes the place to be searched in terms of a rule—in short, for any computer that logs into Playpen, the FBI may deploy the NIT

and retrieve the specified information. However, the fact that any number of individuals potentially could trigger the foregoing rule does not render the NIT warrant any less particular. Instead, the relevant question is whether an officer "can, with reasonable effort ascertain and identify the place intended," if and when the warrant is to be applied. See Blackwood, 913 F.2d at 141 n. 1. The rule as summarized above is precise; it leaves the FBI with no uncertainty in its efforts to "ascertain and identify the place intended." See id. Therefore, to the extent defendant contends that the NIT warrant lacks particularity because it authorizes an indefinite number of searches, defendant's claim is denied.

Finally, the court is aware of no authority, and defendant cites none, to establish that when an investigatory agency can accomplish its goals through a narrower warrant, the Fourth Amendment particularity requirement prohibits it from seeking a broader one. Therefore, where defendant contends that the NIT warrant lacks particularity because the FBI could have sought a warrant to deploy the NIT only after Playpen users actually downloaded or uploaded illegal child pornography rather than upon logging into the site, defendant's claim is denied.

For the foregoing reasons, and based upon the specificity with which the warrant application describes how and where the FBI was authorized to deploy the NIT, defendant's claims based upon the Fourth Amendment's particularity requirement are denied.

D. Rule 41(b)

Before addressing the parties' contentions surrounding Rule 41, the court notes at the outset that an amendment to Rule 41 became effective December 1, 2016. See Fed. R. Crim. P. 41 advisory committee's note to 2016 amendment. The amended Rule 41 states:

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search

> electronic storage media and to seize or copy electronically stored information located within or outside that district if: (A) the district where the media or information is located has been concealed through technological means . . . .

Fed. R. Crim. P. 41(b)(6). The foregoing language was added, in part, for the purpose of granting express authorization for magistrate judges to issue warrants of the type the NIT warrant represents. Id. advisory committee's note to 2016 amendment.

Neither party contends that the current version of Rule 41(b) retroactively may authorize the NIT warrant. Indeed, the Supreme Court has clarified that, where it occasionally declares that certain "watershed" rules of criminal procedure may apply retroactively, see Teague v. Lane, 489 U.S. 288, 311 (1989), such retroactivity may be grounded in rights derived only from the Constitution that pre-exist the Court's articulation of the watershed rule. Danforth v. Minnesota, 552 U.S. 264, 271 (2008). Accordingly, where the 2016 amendments to the Federal Rules of Criminal Procedure do not purport to apply retroactively, and where the current Rule 41(b) clearly does not embrace a Constitutional right that pre-exists the 2016 amendments, the analysis that follows evaluates the validity of the NIT warrant under the Rules in effect February 20, 2015, which is the date the NIT warrant issued.

The version of Rule 41(b) in effect February 20, 2015, specifies five circumstances in which a magistrate judge is authorized to issue a warrant. Under Rule 41(b)

> (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
>
> (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

> (3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
>
> (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both . . .
>
> (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
>
> (A) a United States territory, possession, or commonwealth;
>
> (B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
>
> (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b). Based on this rule, defendant contends that the NIT warrant should not have issued on the theory that a magistrate judge sitting in the Eastern District of Virginia possesses no authority to authorize a search in the Eastern District of North Carolina.

First, because neither defendant nor his property was located in the Eastern District of Virginia when the NIT warrant issued, this case does not involve terrorism, and the seizure involved here does not involve persons or property located outside the jurisdiction of any state or district, Rules 41(b)(1), (3), and (5), respectively, do not apply.

The remaining provisions, Rules 41(b)(2) and (4), arguably support the NIT warrant on the theory that browsing a website constitutes the legal equivalent of a virtual trip to the location of the

website's server. However, while the foregoing analogy has some intuitive appeal, the court is aware of no Fourth Circuit precedent that treats the act of visiting a website as legally equivalent to physically traveling to the location of a website's server. Indeed, it is equally plausible to characterize accessing a website as no more than a form of remote communication wherein both parties remain at their respective physical locations and converse through electrical signals. Nonetheless, where there exists doubt regarding validity of the NIT warrant under Rule 41, the court assumes without deciding that accessing a website does not constitute a virtual trip. Therefore, because Rules 41(b)(2) and (4) each require that a person or property enter the district in which the issuing magistrate judge sits, it follows from the court's assumption that neither rule serves to support the NIT warrant.[3]

Under Fourth Circuit precedent, if a warrant is found to have issued in violation of Rule 41, the court must determine whether the noncompliant action rises to the level of a Fourth Amendment violation. United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2006) ("There are two categories of Rule 41 violations: those involving constitutional violations, and all others."). A Rule 41 violation is constitutional in nature if the action in question violates the Fourth Amendment. See id. (analyzing a violation of Rule 41(d) to determine whether the Fourth Amendment required officers' omitted actions). If the violation is indeed constitutional in nature, evidence obtained pursuant to an improperly issued warrant must be suppressed. United States v. Chaar, 137 F.3d 359, 361 (4th Cir. 1998). If the violation is non-constitutional, suppression is warranted "only when the

[3] The government contends that the NIT warrant is permissible under the virtual trip analogy, which, as set forth above, the court declines in this instance expressly to endorse. Additionally, the government contends that it is possible to characterize the NIT as a tracking device attached to the information itself that users retrieve from Playpen's servers. With regard to the latter argument, the government, similarly, has demonstrated no basis in Fourth Circuit precedent for this characterization of the NIT program. Accordingly, the court's analysis in this part primarily focuses on whether defendant is entitled to suppression under the assumption that the NIT warrant indeed issued in violation of Rule 41.

defendant is prejudiced by the violation . . . or when there is evidence of intentional and deliberate disregard of a provision in the Rule." Simons, 206 F.3d at 403.

Nothing in the record suggests that the magistrate judge's failure to comply with Rule 41 rises to the level of a constitutional violation. Specifically, the extent of the Rule 41 violation assumed here is simply that FBI sought the approval of the NIT warrant from a magistrate judge sitting in the wrong district. That is, had the FBI sought the NIT warrant from a magistrate judge sitting in the Eastern District of North Carolina, Rule 41(b)(1) would have authorized the search at issue since defendant's identifying information resided on his computer located in the Eastern District of North Carolina. See Fed. R. Crim. P. 41(b)(1) (authorizing a magistrate judge to issue warrants to search or seize persons or property located within the district in which the magistrate judge sits).

The foregoing violation, if, indeed, there was one, is not unconstitutional because it amounts to a failure to respect arbitrary geographical lines Congress created by statute in establishing the system of federal judicial districts. While the law requires due regard for geographic boundaries created by statute, violations based on such geographic boundaries cannot rise to the level of unconstitutionality for at least two reasons. First, Article III of the Constitution speaks of "[t]he judicial power of the United States" as a homogeneous and undifferentiated whole. U.S. Const. Art. III § 1. That is, where its text does not contemplate the existence of federal judicial districts, Article III suggests that a violation based on a mistake in selecting a district in which to pursue a warrant does not implicate constitutional law. See id.

Second, the Fourth Amendment imposes two jurisdictional requirements upon any authority exercising power to issue a warrant: the authority must be a magistrate, and the magistrate must be

neutral and detached. Dalia v. United States, 441 U.S. 238, 255 (1979). In addition to the foregoing constitutional requirements, Rule 41 imposes conditions that require a closer geographic connection between evidence of criminal activity and a magistrate judge who would issue a warrant to search or seize such evidence. See Fed. R. Crim. P. 41(b). However, where the geographic requirements of Rule 41 are not contained within nor derived from the Fourth Amendment, a violation of any such geographic requirement is not of constitutional import.

In support of a contrary argument, defendant contends that the Rule 41 violation in issue here is, in fact, constitutional in nature because Rule 41, as incorporated in 28 U.S.C. § 636, partly defines the jurisdiction of federal magistrate judges. That statute provides in relevant part, "[e]ach United States magistrate judge serving under this chapter shall have . . . all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts[.]" 28 U.S.C. § 636(a)(1). Based on the foregoing statute, defendant contends that because the NIT warrant was issued in violation of Rule 41, it follows that the NIT warrant, in effect, was issued without judicial approval.

As set forth above, the jurisdictional rules embodied in the Fourth Amendment comprise the twin requirements that to issue a warrant, the issuing authority must be a magistrate and neutral and detached. Defendant does not challenge the neutrality of the magistrate judge who issued the NIT warrant. Further, the remaining requirement is satisfied simply because the issuing authority was a magistrate judge. Although defendant is correct that, assuming without deciding that the magistrate judge did not have statutory authorization to issue the NIT warrant, defendant has not demonstrated that such a mistake amounts to anything more than a statutory violation for which suppression is not automatically available. See Simons, 206 F.3d at 403.

Upon finding that the Rule 41 violation assumed in this case is non-constitutional, the court must determine whether the FBI deliberately and intentionally disregarded the requirements of Rule 41 or whether defendant was prejudiced by the violation. First, defendant cites no evidence or relevant legal authority to suggest that the FBI or the issuing magistrate judge recklessly disregarded the requirements of Rule 41. Specifically, defendant cites United States v. Levin, 186 F.Supp. 3d 26, 42 (D. Mass 2016), for the proposition that sufficient legal authority existed at the time the FBI sought the NIT warrant to cast doubt upon the proper application of Rule 41 in this case. However, Levin, arising from the same investigation giving rise to this case, was decided well after the FBI sought the NIT warrant; thus, the FBI could not have considered the holding in Levin in choosing a district in which to seek the NIT warrant. Further, Levin cites authority from the D.C. Circuit for the proposition that certain blatant Rule 41 violations may result in suppression, see Levin 186 F.Supp at 42 (citing United States v. Glover, 736 F.3d 509, 515–16 (D.C. Cir 2013). Nonetheless, the facts discussed by the D.C. Circuit in Glover, which involved a defective warrant authorizing use of an audio recording device in a narcotics investigation, are sufficiently distinguishable from the instant matter such that no cause exists to conclude that, when it submitted the NIT warrant application, the FBI knew the NIT warrant would violate Rule 41(b). See Glover, 736 F.3d at 510–11.

Second, as set forth above, the central defect in the NIT warrant that casts doubt upon its validity under Rule 41 is that, arguably, the magistrate judge who issued the NIT warrant sat in the wrong district. Therefore, defendant cannot demonstrate that he suffered prejudice due to this mistake since there is no reason to doubt that a magistrate judge in the Eastern District of North Carolina would have issued the same warrant. Indeed, at the time the NIT warrant issued, there

existed no legal barriers to the FBI's seeking the NIT warrant in every district in the United States, which would have cured the Rule 41 violation that forms the central basis for defendant's Rule 41(b) challenge. It follows, therefore, that had the FBI sought a Rule 41 compliant warrant, defendant would be in the same position in which he finds himself now. Accordingly, where defendant has alleged that the NIT warrant issued in violation of Rule 41, defendant cannot demonstrate prejudice.

In support of a contrary argument, defendant contends that, had the FBI and the issuing magistrate judge complied with Rule 41, the NIT warrant would not have issued, the FBI would not have discovered defendant's identifying information, and, therefore, this case would have ended before it began. Based on this observation, defendant urges the court to find the Rule 41 violation prejudicial. However, defendant's contention ignores the possibility that the FBI could have sought the NIT warrant from the Eastern District of North Carolina, in compliance with Rule 41. Therefore, as set forth above, defendant did not suffer prejudice as a result of the alleged Rule 41 violation.

Because defendant has not demonstrated that the claimed Rule 41 violation at issue is constitutional in nature, intentional or reckless, or prejudicial to defendant's case, defendant's motion to suppress based on alleged violations of Rule 41 is denied.

CONCLUSION

For the foregoing reasons, the court DENIES defendant's motion to suppress. The clerk now will set the matter for arraignment at the court's next regular criminal term no sooner than 45 days from date of entry of this order.

SO ORDERED, this the 28th day of January, 2017.

Louise W. Flanagan

LOUISE W. FLANAGAN
United States District Judge